MTH 411: Final exam, correction
Fall 2015

Exercise 1:
$\mathbb{Q}(\sqrt[3]{2}, \sqrt[5]{3})$ contains the simple extensions $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\sqrt[5]{3})$. These extensions have degree 3 and 5 as the minimal polynomials of $\sqrt[3]{2}$ and $\sqrt[5]{3}$ are $X^3 - 2$ and $X^5 - 3$ respectively. These polynomials are indeed irreducible by Eisenstein criterion for $p = 2$ and $p = 3$ respectively.
Thus the degree $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[5]{3}) : \mathbb{Q}]$ must be divisible by 3 and 5, thus by 15. Now $X^3 - 2$ is a polynomial in $\mathbb{Q}(\sqrt[5]{3})$ with $\sqrt[3]{2}$ as a root, thus $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[5]{3}) : \mathbb{Q}(\sqrt[5]{3})] \leq 5$.
Thus $[\mathbb{Q}(\sqrt[3]{2}, \sqrt[5]{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, \sqrt[5]{3}) : \mathbb{Q}(\sqrt[5]{3})][\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}] \leq 15$.
The degree of the extension is 15.

Exercise 2:
The order of S_p is $p! = p \cdot (p-1) \cdot (p-2) \dots 1$. Thus the highest power of p which divides S_p is p and any subgroup of order p of S_p is a Sylow-p subgroup.
The cyclic group generated by $(123 \dots p)$ has order the order of $(123 \dots p)$ which is p. Thus it is a Sylow-p subgroup.

Exercise 3:
The roots of the polynomial $X^5 - 2$ are the complex numbers $\sqrt[5]{2}e^{\frac{2ik\pi}{5}}$ with $k = 0, 1, 2, 3$ or 4. We can see that $\mathbb{Q}(\sqrt[5]{2}, e^{\frac{2i\pi}{5}})$ contains all these roots, thus $X^5 - 2$ splits over $\mathbb{Q}(\sqrt[5]{2}, e^{\frac{2i\pi}{5}})$.
Furthermore $\mathbb{Q}(\sqrt[5]{2}, \sqrt[5]{2}e^{\frac{2i\pi}{5}})$ contains $e^{\frac{2i\pi}{5}}$ as $e^{\frac{2i\pi}{5}} = \sqrt[5]{2}e^{\frac{2i\pi}{5}} / \sqrt[5]{2}$.
So $\mathbb{Q}(\sqrt[5]{2}, e^{\frac{2i\pi}{5}})$ is generated by the roots of $X^5 - 2$ and thus is the splitting field of $X^5 - 2$.

Problem 1:
1) $P_n(X) = 0 \iff X^n = 1 \iff X = e^{\frac{2ik\pi}{n}}$ for some $k \in \{0, 1, \dots, n-1\}$.

2) $\mathbb{Q}(\omega_n)$ contains all roots of P_n, as $\omega_n^k \in \mathbb{Q}(\omega_n)$. Moreover it is generated over $\mathbb{Q}$ by the roots of P_n, as ω_n already generates $\mathbb{Q}(\omega_n)$. Thus it is the splitting field of $X^n - 1$.

3)Let $\phi : \mathbb{Z}_n \to \mathbb{U}_n$ such that $\phi(k) = \omega_n^k$. ϕ is well defined as $\omega_n^n = 1$. It is obviously surjective, thus bijective as the two group have the same order.
Now ω_n is a generator of $\mathbb{U}_n$ thus ω_n^k is a generator of $\mathbb{U}_n$ if and only if $\exists l$ such that $\omega_n^{kl} = \omega_n \iff kl = 1\ (mod\ n)$.
Then $\exists u, l \in \mathbb{Z}$ such that $kl + un = 1$ which means that $gcd(k, n) = 1$.

4) If $x \in \mathbb{Q}(\omega_n)$ satisfies $x^n - 1 = 0$ then $\varphi(x^n - 1) = \varphi(x)^n - 1 = \varphi(0) = 0$. Thus φ stabilizes the set $\mathbb{U}_n$ of roots of $X^n - 1$.
Furthermore, the restriction of φ to $\mathbb{U}_n$ is a automorphism of the group $\mathbb{U}_n$, thus sends the generator ω_n to some other generator.

5) Let $p(x)$ be the minimal polynomial of ω_n. For any root y of p we know there is an isomorphism of $\mathbb{Q}(\omega_n)$ which sends ω_n to y. Thus y must be a generator of $\mathbb{U}_n$.
Furthermore p is separable as the characteristic of $\mathbb{Q}$ is 0.
Thus the degree of p is at most $\varphi(n)$.

Problem 2:
1) $N(p) = p^2 + 0^2 = p^2$. Assume that p is not irreducible. For any decomposition $p = ab$ into a product of non-units, we must have that $N(a)N(b) = p^2$ and $N(a) \neq 1$ or p^2. Thus $N(a) = p$ and $p \in A$.
On the other hand, if $N(c + di) = p$, then $(c + di)(c - di) = c^2 + d^2 = p$ is a decomposition of p into non-units.

2)We know that the group of units F^* of a finite field F is always cyclic, thus $(\mathbb{Z}_p^*, x)$ is cyclic. Its order is $p - 1 = 4k$.

3)We have that $y^{4k} = 1$ and $y^{2k} \neq 1$ as the order of y is $4k$. Thus y^{2k} is a solution of $x^2 - 1 = 0$ in $\mathbb{Z}_{|}$ which is not 1, thus $y^{2k} = -1$. Thus we have $\left(y^k\right)^2 + 1 = 0 \ (mod\ p)$.

4) We have that $(m + i)(m - i) = m^2 + 1 \in (p)$. But $m \pm i \notin (p)$ as their imaginary part is not divisible by p. Thus the ideal (p) is not prime.

5) $\mathbb{Z}[i]$ is a unique factorization domain. Thus if (p) is not prime then p is not irreducible. Thus $p \in A$ by question 1).